POLICE DEPARTMENT
LEGAL BUREAU
F.O.I.L Unit, Room 110C
One Police Plaza
New York, NY 10038

Emma Best
DEPT MR 56272
411A Highland Ave.
Somerville, MA, 02144

December 4, 2018

FOIL Request #: FOIL-2018-056-03242
Your File #:

Dear Sir or Madam:

This letter is in response to your request received by this office on June 21, 2018 in which you requested access to certain records under the New York State Freedom of Information Law (FOIL).

☑ Responsive to your request, the following document(s) have been accessed and photocopied: **NYPD Patrol Guide Procedure 203-27**

☑ Redactions have been made to the document(s) in that the release of such information would represent an unwarranted invasion of person privacy and would endanger the life and safety of any person {§87.2 (b) and (f)}.

☐ For the following requested item(s), I must refer you to the appropriate agency/agencies or unit that may be in possession of such documents:

☑ In total, ___3__ page(s) have been copied. Please remit payment in the amount of $____Ø____ within thirty (30) days. Failure to do so will result in this file being CLOSED.

☐ The case folder contained records that did not directly pertain to the accident. Such records are not included in the enclosed CD/DVD-ROM.

☑ The requested documents are enclosed with this letter.

☐ Upon receipt of payment, the requested documents will be mailed.

PAYMENT PROCEDURE

Send check or money order (no cash) payable to the **"New York City Police Department"**
Mail payment to:
New York Police Department, F.O.I.L. Unit, Room 110C, One Police Plaza, New York, NY 10038
Note: Please include the FOIL number on the check or money order

APPEAL PROCEDURE

Should you so desire, you may appeal this decision or any portion thereof. Such an appeal must be made in writing, within thirty (30) days of the date of this letter, and must be forwarded to:
Sergeant Jordan S. Mazur, Records Appeals Officer, New York City Police Department, One Police Plaza, Room 1406, New York, NY 10038
Pl or emailed to foilappeals@nypd.orgease include copies of the FOIL request and this letter with your appeal.

Very truly yours,

LT R. Mantellino

Richard Mantellino
Lieutenant
New York City Police Department (NYPD)

PATROL GUIDE

Section: General Regulations		Procedure No: 203-27	
DEPARTMENT EMAIL POLICY			
DATE ISSUED 10/16/18	DATE EFFECTIVE 10/16/18	REVISION NUMBER	PAGE 1 of 3

PURPOSE To inform members of the service of the Department's rights and use policy pertaining to email usage.

PROCEDURE Duties of members of the service creating an email account and using the Department's email system:

MEMBER OF THE SERVICE

1. Review and comply with *A.G. 325-35, "Department Computer Use Policy and Monitoring Notice."*
2. Use Department email system for Department related purposes only.
   a. Use of other email systems (e.g., Gmail, Yahoo, etc.) to conduct Department business is prohibited.
3. Do not use Department email to access or transmit materials (other than those required for police business) that involve the use of obscene language, inappropriate images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals.
4. Do not use the Department email system to create or distribute communications that are offensive, disruptive or unprofessional.
5. Do not use Department email system to conduct personal business.

NOTE *Emails must be drafted with the same level of accuracy and professionalism as any other official Department communication.*

6. Notify integrity control officer/designated supervisor of unauthorized use or receipt of improper content.
7. Notify integrity control officer/designated supervisor of any password compromise or breach of security.
8. Members of the service should check their email at least once a tour.

INTEGRITY CONTROL OFFICER/ DESIGNATED SUPERVISOR

9. Notify Information Technology Bureau (ITB) Service Desk upon notification by a member of command of a breach in password security.
10. Conduct an immediate investigation and take disciplinary action, if necessary, upon receipt of a complaint of misuse of Department email system.
11. Conduct an immediate investigation and comply with *P.G. 205-37, "Sexual, Ethnic, Racial, Religious, or Other Discriminatory Slurs Through Display of Offensive Material"* upon receipt of a complaint of improper content on Department email system.

COMMANDING OFFICER/

12. Ensure all members of command/unit are aware of the Department's email policy.

DESIGNATED SUPERVISOR

13. Notify the command integrity control officer of any unauthorized use or misuse of the Department's email system.

ADDITIONAL DATA

DEPARTMENT EMAIL POLICY NOTICE

Members of the Service are advised that they do not maintain any right to privacy in email communications. All email communications sent or received by Department email are subject to review without notice to the user. Members of the service should understand that any email has the potential to be Rosario material, and may be reviewed by the Department, outside agencies, District Attorneys and Criminal Defense attorneys.

All email communications may be stored and retrieved by the Department, regardless of whether a user intends or attempts to delete sent or received messages from the user's mailbox.

Email communications offer benefits such as speed and efficiency. However, they also present substantial risks because they are frequently prepared and sent quickly and without supervisory review. The facts and information contained in emails may not be as complete or accurate as more formal reports. Emails may reflect a familiar or jovial tone, which may be misinterpreted. Members of the service should exercise the same care in generating emails as they exercise when drafting more formal reports and should only write and send email communications that they would feel comfortable being displayed to a jury or in the media. Members of the service should think about the content of any email before sending it; use appropriate language; and think about whether an email should be sent in the circumstances or whether an alternative form of communication is more appropriate.

All members of the service shall use a confidential password known only to the member of the service to access Department email systems. Members of the service must keep their password secure and not disclose it to another user.

Users are responsible for the transmission of emails from their assigned email accounts and must log off or otherwise secure their account when their workstations are unattended.

All members of the service must provide a signature block at the end of their emails. This signature block must provide name, rank/title and command.

While emails may be sent from shared accounts on an official basis (i.e., [redacted], all such emails must contain a signature block identifying the sender, including name, rank/title and command.

ADDITIONAL DATA (continued)

In addition to the standard signature block, all emails must also contain this concluding banner:

CONFIDENTIALITY NOTICE: This email and any attachments may contain confidential and privileged information for the use of the designated recipient(s) named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, use or disclosure of it or its contents is prohibited and may violate laws including the Electronic Communications Privacy Act. If you are not the inteuded recipient, please contact the sender and destroy all copies of this communication.

Please treat this and all other communications from the New York City Police Department as LAW ENFORCEMENT SENSITIVE/FOR OFFICIAL USE ONLY.

For assistance with email login, including password reset or address name change, members of the service should contact the Information Technology Bureau Service Desk.

Confidential information, including information requiring compliance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information System (CJIS), should not be shared via email. CJIS data includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data.

The electronic transmission of intelligence files and information containing sensitive tactical and undercover information is prohibited.

Shortened URLs are unauthorized in any part of an email message (i.e., hyperlinks shortened using a third party URL shortener, including tinyurl.com; bit.ly.; goo.gl, etc.). Members of the service should refer to A.G. 325-47, "Cyber Security Incidents" regarding suspected or actual cyber security incidents affecting NYPD information systems or electronic information assets. Questions regarding the security of Department email accounts and reports of security incidents (e.g., phishing, suspicious attachments) should be directed to the Information Technology Bureau, Information Security Office at [redacted].

As a reminder, the Information Technology Bureau will never ask for any personal information or provide any links in a generic email. Emails claiming to be sent by the Information Technology Bureau Service Desk or administrators directing the user to a website or asking for specific information should not be answered. The security verification will be located at the very beginning of the message and shall contain the rank, command, name and last three digits of Tax ID number.

RELATED PROCEDURES

FINEST Communication System (A.G. 322-04)
Department Computer Use Policy and Monitoring Notice (A.G. 325-35)
Department Computer Systems (P.G. 219-14)
Cyber Security Incidents (A.G. 325-47)
Department Computer Systems – Password (A.G. 325-44)
Sexual, Ethnic, Racial, Religious, or Other Discriminatory Slurs Through Display of Offensive Material (P.G. 205-37)